

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

JASON BRAUN and STEPHANIE
CARTER, on behalf of themselves and all
others similarly situated,

Plaintiffs,

v.

THE PHILADELPHIA INQUIRER, LLC,

Defendant.

Master File Case No. 2:22-cv-04185-JMY

**CONSOLIDATED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Jason Braun and Stephanie Carter, on behalf of themselves and all others similarly situated, file this Complaint against Defendant The Philadelphia Inquirer, LLC, (“Defendant”) for violation of the federal Video Privacy Protection Act, 18 U.S.C. § 2710 (“VPPA”) and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701 *et seq.* (“Pennsylvania Wiretap Act”). Plaintiffs’ allegations are made on personal knowledge as to Plaintiffs and their own acts and upon information and belief as to all other matters.

I. NATURE OF THE ACTION

1. This is a consumer class action complaint against Defendant as the owner and operator of the Inquirer.com website for violating the VPPA and the Pennsylvania Wiretap Act.

By deciding to use Facebook’s Meta Pixel on its website, Defendant knowingly intercepted Subscribers’ (“Subscribers” refers to persons with digital subscriptions to Inquirer.com) electronic communications without the proper consent. Defendant then disclosed to Facebook the contents of these electronic communications in the form of Subscribers’ (i) personally identifiable Facebook ID (“FID”) and (ii) the computer file containing the watched video and its corresponding URL (the “uniform resource locator” or web address) (“Video Media”). Together, the FID and Video Media constitute a Subscriber’s “Personal Viewing Information.”

2. Defendant serves video content to tens of thousands of subscribers to its Inquirer.com website throughout the United States. Subscribers can view exclusive video content via the Inquirer.com website or mobile application (the “App”) on their mobile devices.

3. Defendant collects and shares the personal information of visitors to its website and App with third parties. Defendant does this in a number of ways, including using cookies (small blocks of data stored on an internet user’s computer to track the user’s browsing activity); software development kits, or “SDKs” (sets of software and tools allowing developers to create applications); and pixels (pieces of code installed on website that measure the actions users take on a website).

4. The Meta Pixel (f/k/a Facebook Pixel) is a code Defendant installed on its website allowing Defendant to track “conversions”—that is, when users take certain actions on its website, such as clicking an ad or viewing content—and to collect users’ data. More specifically, the Meta Pixel allows Defendant to track when a Subscriber visits the Inquirer.com website or App and views Video Media, as well as the Subscriber’s FID.

5. Importantly, without Subscriber consent, Defendant discloses the Subscriber’s Personal Viewing Information—i.e., Subscriber’s unique FID and video content viewed—*together*

as one data point to Facebook. Because the Subscriber’s FID uniquely identifies an individual’s Facebook user account, Facebook—or any other ordinary person—can use it to quickly and easily locate, access, and view a Subscriber’s corresponding Facebook profile. Put simply, the Meta Pixel allows Facebook to know what Video Media a Subscriber viewed on the Inquirer.com website or App.

6. By using the Meta Pixel to track Subscribers’ activity on its website, Defendant targets advertising and other content on its website, and Defendant profits handsomely from its unauthorized interception and disclosure of Personal Viewing Information to Facebook. It does so at the expense of its Subscribers’ privacy and their statutory rights under the VPPA and the Pennsylvania Wiretap Act.

7. The VPPA prohibits video tape service providers from knowingly disclosing consumers’ personally identifiable information, including “information which identifies a person as having requested or obtained specific video materials or services from a video tape provider,” without express consent in a stand-alone consent form.

8. The VPPA defines “video tape service provider” as anyone “engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” As the owner of Inquirer.com, Defendant is engaged in the delivery of such audio visual materials.

9. Section 5703 of the Pennsylvania Wiretap Act prohibits: (1) intentional interception, endeavors to intercept, and procurement of any other person to intercept or endeavor to intercept any wire, electronic or oral communication; (2) intentional disclosure or endeavors to disclose the contents of such wire, electronic, or oral communications, knowing or having reason to know that the information was obtained through interception; and (3) the intentional use or

endeavors to use the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through interception. Defendant's integration of the Meta Pixel on its website to track Subscribers' Personal Viewing Information constitutes the interception of Subscribers' electronic communications and the disclosure and use of the contents of those electronic communications.

10. Because Defendant's Subscribers are not informed about this dissemination of their Personal Viewing Information – indeed, it is automatic and *invisible* – they do not consent and cannot exercise reasonable judgment to defend themselves against the highly personal ways Defendant has used and continues to use their data to make money for itself.

11. Defendant chose to disregard Plaintiffs' and other Subscribers' statutorily protected privacy rights by releasing their personal data to Facebook. Accordingly, Plaintiffs bring this class action for legal and equitable remedies to redress and put a stop to Defendant's practices of intentionally intercepting and disclosing its Subscribers' Personal Viewing Information to Facebook in knowing violation of the VPPA and the Pennsylvania Wiretap Act.

II. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Video Privacy Protection Act, 18 U.S.C. § 2710. This Court also has supplemental jurisdiction over the claims arising under the Pennsylvania Wiretap Act, 18 Pa. C.S. § 5701 *et seq.*, pursuant to 28 U.S.C. § 1367.

13. Venue is appropriate in the Eastern District of Pennsylvania pursuant to 28 U.S.C. § 1391 because both Plaintiff and Defendant reside in this District and Defendant does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

III. PARTIES

14. Plaintiff Jason Braun is an adult citizen of Lafayette Hill, Pennsylvania. Plaintiff Braun has had a paid digital subscription to Inquirer.com since no later than 2012, and, in the past, maintained a traditional print subscription to The Philadelphia Inquirer beginning in or around 1997. Plaintiff Braun has had a Facebook account since at least 2008 which he regularly accesses using his laptop, desktop, and smartphone. During the relevant time period, Plaintiff Braun accessed his Inquirer.com digital subscription on his laptop, desktop, and smartphone to request and view Video Media through the Inquirer.com website and/or App. By doing so, Plaintiff Braun's Personal Viewing Information was disclosed to Facebook pursuant to the systematic process described herein. Plaintiff Braun never gave Defendant express written consent to disclose his Personal Viewing Information.

15. Plaintiff Stephanie Carter is an adult citizen of Philadelphia, Pennsylvania. Plaintiff Carter began her paid digital subscription to Inquirer.com around 2017 and maintains the subscription to this day. Plaintiff Carter has had a Facebook account from at least 2012 to the present, which she regularly accesses using her computer and smartphone. During the relevant time period, Plaintiff Carter accessed her Inquirer.com digital subscription on her computer and smartphone to request and view Video Media through the Inquirer.com website and/or App. By doing so, Plaintiff Carter's Personal Viewing Information was disclosed to Facebook pursuant to the systematic process described herein. Plaintiff Carter never gave Defendant express written consent to disclose her Personal Viewing Information.

16. Defendant The Philadelphia Inquirer, LLC, is a media company and owner of The Philadelphia Inquirer newspaper and the Inquirer.com website. Defendant is a public benefit corporation with its principal place of business located in Philadelphia, Pennsylvania. As detailed

below, through the Inquirer.com website and App, Defendant delivers countless hours of video content to its paid Subscribers.

IV. FACTUAL ALLEGATIONS

A. The Video Privacy Protection Act

17. The VPPA generally prohibits the knowing disclosure of a customer's video rental or sale records without the informed, written consent of the customer in a form "distinct and separate from any form setting forth other legal or financial obligations." Under the statute, the Court may award actual damages (but not less than liquidated damages of \$2,500.00 per person), punitive damages, equitable relief, and attorneys' fees.

18. The VPPA was initially passed in 1988 for the explicit purpose of protecting the privacy of individuals' and their families' video rental, purchase, and viewing data. Leading up to its enactment, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." S. Rep. No. 100-599 at 7-8 (1988).

19. Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audio visual materials. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

20. In proposing the Video and Library Privacy Protection Act (later codified as the VPPA), Senator Leahy stated that "[i]n practical terms our right to privacy protects the choice of

movies that we watch with our family in our own homes. And it protects the selection of books that we choose to read.” 134 Cong. Rec. S5399 (May 10, 1988). Thus, the personal nature of such information, and the need to protect it from disclosure, is the inspiration of the statute: “[t]hese activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people.” *Id.*

21. While these statements rang true in 1988 when the VPPA was passed, the importance of legislation like the VPPA in the modern era of data mining from online activities is more pronounced than ever before. During a 2012 Senate Judiciary Committee meeting, “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century,” Senator Leahy emphasized the point by stating: “While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other new technologies have revolutionized the availability of Americans’ information.”¹

22. In this case, Defendant chose to deprive Plaintiffs and Class members of that right by systematically disclosing their Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) anyone, as explained herein.

B. Pennsylvania’s Wiretapping and Electronic Surveillance Control Act

23. The Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701 *et seq.* (“Pennsylvania Wiretap Act”) offers a civil cause of action to “any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation of”

¹ The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, <https://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century> (last accessed Oct. 31, 2022).

the statute, against “any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication.” 18 Pa. C.S. § 5725(a).

24. The Pennsylvania Wiretap Act is generally modeled after the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, which provides uniform minimum protections for wire, electronic, and oral communications, and which authorizes states to adopt wiretap statutes that provide greater—but not lesser—protection than what is available under federal law.

25. The principal focus and purpose of the statute is the protection of privacy, and therefore its provisions must be strictly construed.

26. Defendant violated the Pennsylvania Wiretap Act by intentionally procuring the Meta Pixel to intercept Plaintiffs’ electronic communications and by using the content of those communications for Defendant’s own purposes, such as tracking website usage and advertising.

C. Inquirer.com Digital Subscriptions

27. Defendant owns The Philadelphia Inquirer. Founded in 1829, The Philadelphia Inquirer is the third longest continually operating daily newspaper in the United States.

28. People who wish to access The Philadelphia Inquirer’s content online may do so by paying for a subscription to Inquirer.com.

29. On information and belief, all Subscribers to Inquirer.com provide Defendant with their IP (Internet Protocol) address, which is a unique number assigned to any device connected to the internet or a local network, that informs Defendant as to Subscribers’ city, zip code and physical location. Subscribers may also provide to Defendant the identifier on their mobile devices and/or cookies stored on their devices.

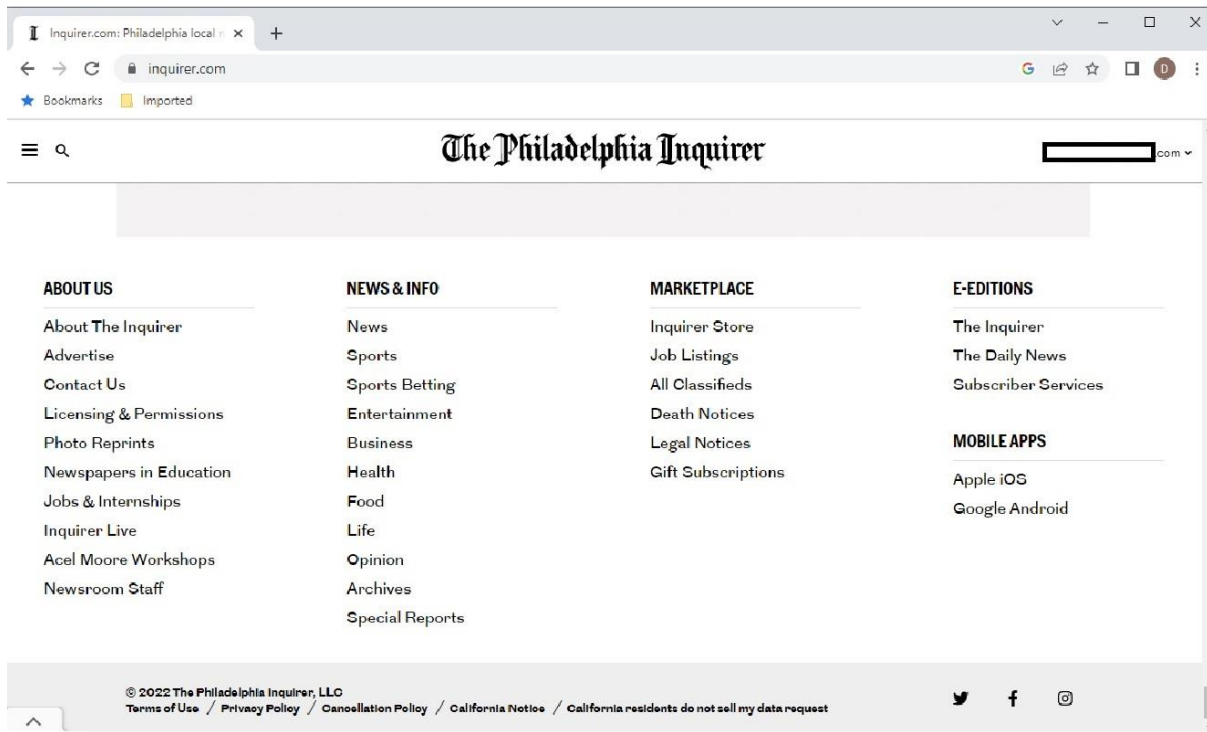
30. When a Subscriber opens an account, Defendant does not disclose that it will share their Personal Viewing Information with third parties, such as Facebook. Subscribers are also not

asked to consent to such information sharing.

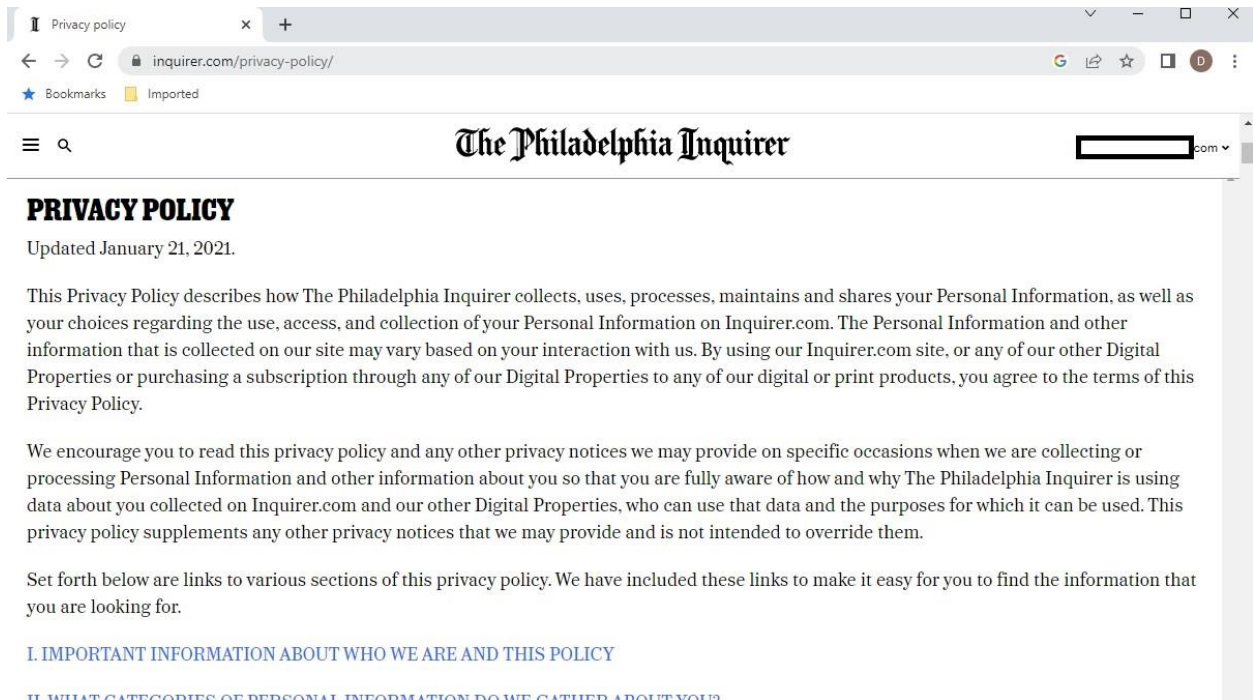
31. Inquirer.com Subscribers have access to a variety of Video Media on Defendant's digital platform. Notably, once a Subscriber signs in and watches Inquirer.com Video Media, he or she is not provided with any notification that their Personal Viewing Information is being given to Facebook. Similarly, Defendant also fails to obtain Subscribers' written consent to collect their Personal Viewing Information "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer," as the VPPA requires.

D. Defendant Admits It May Collect Digital Subscribers' Information But Fails to Inform Subscribers or Obtain Their Consent to Share Personal Viewing Information

32. A Subscriber or any other visitor to Inquirer.com must scroll to the very bottom of the home page, passing the equivalent of approximately 9 printed 8.5"x11" pages, to reach a list of 5 inconspicuous hyperlinks, including the Privacy Policy:



33. A Subscriber or any other visitor clicking on the Privacy Policy hyperlink is taken to the page below:



34. The Privacy Policy states that when a Subscriber uses Inquirer.com’s services, Defendant may “collect, use, store, and transfer different kinds of Personal Information about you” such as **Identity Data**, Contact Data, Financial Data, Transaction Data, Mobile Device Location Data, **Usage Data**, Profile Data, Marketing and Communications Data, and Technical Data.²

35. The Privacy Policy describes **Identity Data** as including “first name, maiden name, last name, **username or similar identifier**, birth year, gender, marital status, title or basic demographic information.” Usage Data includes “information about how you use our Digital Properties and Services.”³

36. Defendant states it allows “certain third parties advertising on our site to collect

² Privacy Policy, updated Jan. 21, 2021, available at <https://www.inquirer.com/privacy-policy/> (last visited Oct. 31, 2022) (emphasis added).

³ *Id.* (emphasis added).

certain Personal Information about you on our site, **but that data does not include identity, contact or financial data as described above**, and to use that data for marketing and other legitimate business purposes.”⁴

37. In other words, Defendant states that it *does not* allow third parties like Facebook to collect Subscribers’ “Identity Data,” which Defendant itself defines to include “username or other identifier.”

38. Importantly, nowhere in the Inquirer Privacy Policy is it disclosed that Defendant will intercept Subscribers’ private and protected Personal Viewing Information and share it with Facebook or other third parties. Moreover, Defendant does not obtain Subscribers’ written consent to collect their Personal Viewing Information “in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer,” as required by the VPPA.

E. How Inquirer.com Intercepts, Discloses, and Uses Digital Subscribers’ Personal Viewing Information

1. Tracking Pixels

39. Websites and apps that choose to use the Meta Pixel are aware that it collects information about user’s devices and activities and sends that information to Facebook. Facebook then uses that information to send targeted ads to the user.

40. The Meta Pixel, also known as a “tag” or “web beacon” among other names, is an *invisible* tool that tracks consumers’ actions on Facebook advertisers’ websites and reports them to Facebook. It is a version of the social plugin that gets “rendered” with code from Facebook. To obtain the code for the Meta Pixel, the website advertiser tells Facebook which website events it wants to track (e.g., Video Media) and Facebook returns corresponding Facebook pixel code for the advertiser to incorporate into its website.

⁴ *Id.* (emphasis added).

41. Defendant installed the Meta Pixel, which enables it to intercept and disclose Plaintiffs' and Class Members' Personal Viewing Information to Facebook, because it benefits financially from the advertising and analytics services that stem from use of the Metal Pixel. When a Subscriber visits the Inquirer.com website, Defendant sends to Facebook certain information about the Subscriber, including, but not limited to, their identity and the media content the Subscriber watched. Specifically, Inquirer.com sends to Facebook the video content name, its URL, and, most notably, the Subscriber's Facebook ID.

2. Facebook ID ("FID") and Video Media

42. The Facebook ID ("FID") is a unique and persistent identifier that Facebook assigns to each user. As Facebook itself explains, any ordinary person can look up the user's Facebook profile and name using the FID:

User ID

Your User ID is a string of numbers that doesn't personally identify you but does connect to your Facebook profile. You have a User ID automatically, whether or not you choose to create a username. Learn how to [find your user ID](#).

User IDs can:

- Allow someone with the ID to see your profile, including any public information. Learn how to [adjust what people can see in your profile](#).
- Help other applications personalize your experience by connecting with your Facebook account. When you allow apps to connect with your Facebook account, they can use your user ID to see public information, like your public profile and your friend list.
- When you run into issues with an app or game, your User ID can help the developer better investigate the problem to understand and address your specific concerns.

43. When a Facebook user with one or more personally identifiable FID cookies on their browser views Video Media on the Inquirer.com website or App, Defendant, through use of the Meta Pixel, causes the Subscriber's identity and Personal Viewing Information to be transmitted to Facebook via Subscriber's browser. This transmission is not the Subscriber's

decision, but results from Defendant's purposeful use of the Meta Pixel by incorporation of that pixel and code into Defendant's website and App.

44. Defendant could easily program the website and App so that this information is not automatically transmitted to Facebook when a Subscriber views Video Media. However, it is not in Defendant's financial interest to do so because Defendant benefits financially from using the Meta Pixel. The Meta Pixel allows companies like Defendant to track conversions from Facebook ads (e.g., track who visits Inquirer.com by clicking on a Facebook ad), optimize ads, and build targeted audiences for future ads.

45. Any individual on Facebook can be easily identified with only their unique FID. Facebook admits this on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile. Simply put, with only an FID, and the video content name and URL—all of which Defendant knowingly and readily provides to Facebook without any consent from the Subscribers—any ordinary person could learn the identity of the Subscriber and the specific video or media content they requested on Inquirer.com or the App.

F. The Inquirer Unlawfully Causes Facebook to Intercept Digital Subscribers' Personal Viewing Information and Discloses it to Facebook

46. At all relevant times, Defendant procured Facebook to intercept Subscribers' electronic communications through the incorporation of the Meta Pixel on Defendant's website and its App. At all relevant times, Defendant knowingly disclosed Personal Viewing Information to Facebook through the Meta Pixel. This is evidenced by, among other things, the functionality of the Meta Pixel, including that it enabled Defendant to show targeted advertising to its Subscribers based on the Video Media those Subscribers had previously viewed on the Inquirer website or App. Defendant receives a financial benefit from the advertising facilitated by the Meta Pixel.

47. Upon information and belief, Defendant maintains a vast digital database

comprised of its Subscribers' Personal Viewing Information, including the names and e-mail addresses of each Subscriber and information reflecting the Video Media that each of its Subscribers viewed.

48. Defendant is not sharing anonymized, non-personally identifiable data with Facebook. To the contrary, the data it discloses is tied to unique identifiers that track specific Facebook users. Importantly, the recipient of the Personal Viewing Information—Facebook—*receives the Personal Viewing Information as one data point*. Defendant has thus monetized its database by disclosing its Subscribers' Personal Viewing Information to Facebook in a manner allowing it to make a direct connection—without the consent of its Subscribers and to the detriment of their legally protected privacy rights.

49. Critically, the Personal Viewing Information Defendant intercepts and discloses to Facebook allows Facebook to build from scratch or cross-reference and add to the data it already has in its own detailed profiles for its own users, adding to its trove of personally identifiable data.

50. These factual allegations are corroborated by publicly available evidence. When an Inquirer.com Subscriber clicks on an article and watches a video, Defendant sends certain information to Facebook.

51. For example, when a Subscriber clicked and watched a video titled “These South Philly mural tell Latino immigrants’ stories,” Defendant sent that video’s title, the URL, and the digital Subscriber’s FID (as the cookie “c_user”), along with other data, to Facebook:

The screenshot shows a web browser displaying a news article on 'The Inquirer' website. The article is titled 'These South Philly murals tell Latino immigrants' stories' and includes a quote from Lemus, a first-generation Mexican American and the arts and education coordinator at Puentes de Salud. Below the article is a video player showing a mural. The browser's developer tools are open, showing the Network tab with a list of requests. The selected request is from 'facebook' to 'fafacebook.svg'. The 'Request Headers' section is expanded, showing the following details:

- Authority:** www.facebook.com
- Method:** GET
- Path:** /tr/?id=1728487820781559&ev=PageView&dl=https%3A%2F%2Fwww.inquirer.com%2Fnews%2Fsouth-philly-murals-showcase-immigrant-stories-20221027.html&r1=https%3A%2F%2Fwww.inquirer.com%2Fnews%2F&if=false&ts=1666897484831&sw=1440&sh=900&v=2.9.88&r=stable&ec=2&o=30&fbp=fb.1.166256399728.209825932&it=1666897464778&coo=false&rqm=GET
- Scheme:** https
- Accept:** image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
- Accept-Encoding:** gzip, deflate, br
- Accept-Language:** en-US,en;q=0.9
- Cookie:** sb=GtilyV7ZYe3WkNAXGLPLr17n; datr=AXyWYWFWeWgVE4vBR-nRYjHv; c_user=67[redacted] xs=45%3ADNDGYWo5oUd9TQ%3A2%3A1655833290%3A-1%3A3026%3A%3AAcWnLakfsVDpHq6vgOtUIVUD1pFdxXuyNT0-KCCkIU; f=r=0EUcutQhAu3izuUuG.AWWRX817EOKxEg5N4cKlH88zXzw.BjWstJ.01.AAA.0.0.BjWstJ.AWUfk0FQ2E4
- Referer:** https://www.inquirer.com/
- Sec-CH-UA:** "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"

This block provides a detailed view of the 'Request Headers' for the selected network request. The headers are as follows:

- strict-transport-security:** max-age=31536000; includeSubDomains
- Request Headers:**
 - authority:** www.facebook.com
 - method:** GET
 - path:** /tr/?id=1728487820781559&ev=PageView&dl=https%3A%2F%2Fwww.inquirer.com%2Fnews%2Fsouth-philly-murals-showcase-immigrant-stories-20221027.html&r1=https%3A%2F%2Fwww.inquirer.com%2Fnews%2F&if=false&ts=1666897484831&sw=1440&sh=900&v=2.9.88&r=stable&ec=2&o=30&fbp=fb.1.166256399728.209825932&it=1666897464778&coo=false&rqm=GET
 - scheme:** https
 - accept:** image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
 - accept-encoding:** gzip, deflate, br
 - accept-language:** en-US,en;q=0.9
 - cookie:** sb=GtilyV7ZYe3WkNAXGLPLr17n; datr=AXyWYWFWeWgVE4vBR-nRYjHv; c_user=67[redacted] xs=45%3ADNDGYWo5oUd9TQ%3A2%3A1655833290%3A-1%3A3026%3A%3AAcWnLakfsVDpHq6vgOtUIVUD1pFdxXuyNT0-KCCkIU; f=r=0EUcutQhAu3izuUuG.AWWRX817EOKxEg5N4cKlH88zXzw.BjWstJ.01.AAA.0.0.BjWstJ.AWUfk0FQ2E4
 - referer:** https://www.inquirer.com/
 - sec-ch-ua:** "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"

52. The “c_user” cookie, or FID, is a unique identifier of the Facebook user currently logged onto Facebook on that device. An ordinary person who knows a Facebook user’s FID can easily look up the Facebook user’s Facebook profile by entering “www.facebook.com/[insert

FID]”. Importantly, any ordinary person who searches the FID on the internet can easily identify the person who is associated with the FID on Facebook.

53. As a result of Defendant’s data compiling and sharing practices, Defendant has knowingly disclosed to Facebook for its own personal profit the Personal Viewing Information of Defendant’s Subscribers, together with additional personal information.

54. Defendant does not seek its Subscribers’ consent to the disclosure of their Personal Viewing Information (in writing or otherwise) and its customers remain unaware that their Personal Viewing Information and other sensitive data is being disclosed to Facebook.

55. By disclosing its Subscribers Personal Viewing Information to Facebook— which undeniably reveals both an individual’s identity and the specific video materials they requested from Defendant’s website —Defendant has intentionally and knowingly violated the VPPA and Pennsylvania Wiretap Act.

G. Intercepting Electronic Communications and Disclosing Personal Viewing Information is Not Necessary for Defendant’s Business.

56. Tracking pixels are not necessary for Defendant to operate Inquirer.com’s digital news publications and sign-up digital subscribers. This tracking software is deployed on Defendant’s website and App for the sole purposes of intercepting electronic communications to enrich Defendant and Facebook.

57. Even if an on-line news publication found it useful to integrate Facebook tracking pixels, Defendant is not required to disclose Personal Viewing Information to Facebook. In any event, if Defendant wanted to do so, it must first comply with the strict consent requirements of the VPPA and the Pennsylvania Wiretap Act, which it failed to do.

H. Plaintiffs’ Experiences

58. Plaintiff Jason Braun became a digital Subscriber to Inquirer.com by providing,

among other information, his name, address, email address, IP address (which informs Defendant as to the city and zip code in which a Subscriber resides in as well as their physical location), and any cookies associated with his device(s). Plaintiff Braun pays for his Inquirer.com subscription and receives emails and other news alerts from Defendant in conjunction with this subscription.

59. Plaintiff Stephanie Carter has been a paid Inquirer.com Subscriber from approximately 2017 through the present. Plaintiff initially subscribed to the website by providing, among other information, her name, address, her email address, IP address (which informs Defendant as to the city and zip code in which a Subscriber resides as well as their physical location), and any cookies associated with her device(s). As part of this subscription, Plaintiff receives emails and other news from Defendant.

60. Since no later than 2012, Plaintiff Braun has used his laptop, desktop, and smartphone to view Video Media on Inquirer.com and, as an avid sports fan, recalls watching sports-related videos.

61. Plaintiff Braun has had a Facebook account since at least 2008, which he regularly accesses from his laptop, desktop, and smartphone. His Facebook account contains additional personal information and other personal details.

62. From approximately 2017 to the present, Plaintiff Carter has viewed Video Media on Inquirer.com from her computer and smartphone. She recalls viewing videos related to news articles and consumer issues.

63. Plaintiff Carter has had a Facebook account since approximately 2012 through the present. She accesses her Facebook account via her computer and mobile device. Her Facebook account contains additional personal information and other personal details.

64. Plaintiffs Braun and Carter never consented to, authorized, or otherwise permitted

Defendant to intercept their electronic communications or disclose their Personal Viewing Information to Facebook. Plaintiffs Braun and Carter did not provide informed written consent to such disclosures in a form distinct and separate from any form setting forth their other legal obligations. Defendant did not provide a clear and conspicuous opportunity for Plaintiffs to withdraw from or opt out of these disclosures. Nevertheless, Defendant knowingly shared Plaintiffs' Personal Viewing Information with Facebook.

V. CLASS ACTION ALLEGATIONS

65. Plaintiffs brings a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and all others similarly situated (the "Class"):

All persons in the United States with digital subscriptions to Inquirer.com who viewed Video Media on Defendant's website or App and used Facebook during the time the Meta Pixel was active on Defendant's website or App.

66. Excluded from the Class are Defendant, its past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

67. Numerosity. Members of the Class are so numerous and geographically dispersed that joinder of all members of the Class is impracticable. Plaintiffs believe that there are potentially tens of thousands of members of the Class widely dispersed throughout the United States. Class members can be identified from Defendant's records and non-party Facebook's records.

68. Typicality. Plaintiffs' claims are typical of the claims of members of the Class. Plaintiffs and members of the Class were harmed by the same wrongful conduct by Defendant in that Defendant caused Personal Viewing Information to be disclosed to Facebook without obtaining express written consent. Their claims are based on the same legal theories as the claims

of other Class members.

69. Adequacy. Plaintiffs will fairly and adequately protect and represent the interests of the members of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiffs are represented by counsel with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically.

70. Commonality. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class because Defendant has acted on grounds generally applicable to the Class. Questions of law and fact common to the Class include:

- a. Whether Defendant knowingly disclosed Class members' Personal Viewing Information to Facebook;
- b. Whether the information disclosed to Facebook concerning Class members' Personal Viewing Information constitutes personally identifiable information under the VPPA;
- c. Whether Defendant's disclosure of Class members' Personal Viewing Information to Facebook was knowing under the VPPA;
- d. Whether Class members consented to Defendant's disclosure of their Personal Viewing Information to Facebook in the manner required by 18 U.S.C. § 2710(b)(2)(B);
- e. Whether Defendant intentionally intercepted or procured another person to intercept Class members' electronic communications in violation of the Pennsylvania Wiretap Act;
- f. Whether Defendant intentionally disclosed the contents of Class members'

electronic communications;

g. Whether Defendant intentionally used the contents of Class members'

electronic communications; and

h. Whether the Class is entitled to damages and other relief as a result of Defendant's conduct.

71. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs know of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

VI. TOLLING OF STATUTES OF LIMITATIONS

72. Applicable statutes of limitations have been tolled by Defendant's knowing and active concealment of the facts alleged herein. Plaintiffs and Class members could not have reasonably discovered Defendant's practices of sharing their Personal Viewing Information with Facebook until shortly before this litigation commenced.

73. Defendant was and remains under a continuing duty to disclose to Plaintiffs and Class members its practices of sharing Personal Viewing Information with Facebook. As a result of the active concealment by Defendant, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Violation of the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710

74. Plaintiffs incorporate the preceding paragraphs by reference as if fully set forth herein and bring this claim individually and on behalf of the Class.

75. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally-identifying information” concerning any consumer to a third-party without the “informed, written consent (including through an electronic means using the Internet) of the consumer.” 18 U.S.C. § 2710.

76. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials.”

77. Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes, and those sales affect interstate or foreign commerce.

78. As defined in 18 U.S.C. § 2710(a)(3), “personally-identifiable information” is defined to include “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.”

79. Defendant knowingly caused the Personal Viewing Information, including FIDs, of Plaintiffs and Class members to be disclosed to Facebook. This information constitutes personally identifiable information under 18 U.S.C. §2710(a)(3) because it identified each Plaintiff and Class member to Facebook as an individual who viewed Inquirer.com Video Media, including the specific video materials requested from the website.

80. As defined in 18 U.S.C. § 2710(a)(1), a “consumer” is “any renter, purchaser, or subscriber of goods or services from a video tape service provider.” As alleged *supra*, Plaintiffs subscribed to Inquirer.com, which provides Video Media content to Subscribers’ desktops, tablets, and mobile devices. Plaintiffs are thus “consumers” under this definition.

81. As set forth in 18 U.S.C. § 2710(b)(2)(B), “informed, written consent” must be (1) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; and (2) at the election of the consumer, is either given at the time the disclosure is sought or given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner.” Defendant failed to obtain informed, written consent under this definition.

82. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). Video tape service providers must “provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer’s election.” Defendant failed to provide an opportunity to opt out as required by the VPPA.

83. Defendant knew that these disclosures identified Plaintiffs and Class members to Facebook. Defendant also knew that Plaintiffs’ and Class members’ Personal Viewing Information was disclosed to Facebook because, *inter alia*, Defendant chose, programmed, and intended for Facebook to receive the video content name, its URL, and, most notably, the Subscribers’ FID.

84. By disclosing Plaintiffs’ and the Class’s Personal Viewing Information, Defendant violated Plaintiffs’ and the Class members’ statutorily protected right to privacy in their video-watching habits. *See* 18 U.S.C. § 2710(c).

85. As a result of the above violations, Defendant is liable to the Plaintiffs and other Class members for actual damages related to their loss of privacy in an amount to be determined

at trial, or alternatively for “liquidated damages not less than \$2,500 per plaintiff.” Under the VPPA, Defendant is also liable for reasonable attorney’s fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CLAIM FOR RELIEF

**Violation of the Pennsylvania Wiretapping and Electronic Surveillance
Control Act, 18 Pa. C.S. § 5701 *et seq.***

86. Plaintiffs incorporate the preceding paragraphs by reference as if fully set forth herein and bring this claim individually and on behalf of the Class.

87. The Pennsylvania Wiretap Act prohibits the (1) intentional interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication.

88. By visiting Defendant’s website and viewing videos, Plaintiffs and Class members engaged in electronic communications with Defendant.

89. Plaintiffs and Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

90. Plaintiffs and Class members did not consent to having their electronic communications with Defendant intercepted by Facebook.

91. Defendant procured Facebook to automatically and surreptitiously intercept Plaintiffs’ and Class members’ electronic communications in real-time by installing the Meta Pixel

on its website.

92. Defendant intentionally disclosed to Facebook the contents of Plaintiffs' and Class members' electronic communications in the form of their viewing histories and FIDs and had reason to know that this information was obtained through its interception of such electronic communications.

93. Upon information and belief, Defendant intentionally used Plaintiffs' and Class members' intercepted electronic communications obtained via the Meta Pixel to track Subscribers' activity on Defendant's website.

94. Upon information and belief, Defendant knew that Facebook would add Plaintiffs' and Class members' viewing histories and FIDs to Facebook's own back-end database for advertising, research, product development, and other purposes.

95. As a result of the above violations, Defendant is liable to Plaintiffs and the Class for (1) actual damages, not less than liquated damages computed at the rate of \$100/day for each violation, or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorney's fees and other litigation costs.

VIII. RELIEF REQUESTED

96. Accordingly, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an order:

- a. Certifying this action as a class action pursuant to Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, and direct that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the Class, and declare Plaintiffs as the representatives of the Class;
- b. Declaring that Defendant's conduct as described herein violates the federal VPPA,

18 U.S.C. § 2710(c)(2)(D);

- c. Declaring that Defendant's conduct as described herein violates the Pennsylvania Wiretap Act, 18 Pa. C.S. § 5710 *et seq.*;
- d. Requiring Defendant to pay \$2,500.00 to Plaintiffs and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);
- e. Requiring Defendant to pay damages of \$100 a day for each day of violation, or \$1,000 to Plaintiffs and each Class member, as provided by the Pennsylvania Wiretap Act, 18 Pa. C.S. § 5725(a);
- f. Awarding punitive damages, as warranted, in an amount to be determined;
- g. Awarding prejudgment interest on all amounts awarded;
- h. Awarding restitution and all other forms of equitable monetary relief;
- i. Issuing injunctive relief as pleaded or as the Court may deem proper;
- j. Awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit; and
- k. Awarding such other relief as the Court deems necessary.

IX. JURY DEMAND

97. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs, on behalf of themselves and the proposed Class, demands a trial by jury on all issues so triable.

Date: February 17, 2023

Respectfully submitted,

/s/ John A. Macoretta

John A. Macoretta (PA 60094)

Jeffrey L. Kodroff (PA 55780)

Diana J. Zinser (PA 203449)

SPECTOR ROSEMAN AND KODROFF, P.C.

2001 Market Street, Suite 3420

Philadelphia, PA 19103

Phone: (215) 496-0300

jmacoretta@srkattorneys.com

jkodroff@srkattorneys.com

dzinser@srkattorneys.com

Jeffrey S. Goldenberg

GOLDENBERG SCHNEIDER, L.P.A.

4445 Lake Forest Drive, Suite 490

Cincinnati, OH 45242

Phone: (513) 345-8291

jgoldenberg@gs-legal.com

tnaylor@gs-legal.com

*Attorneys for Plaintiff Carter and the
Proposed Class*

Gary M. Klinger

MILBERG COLEMAN BRYSON PHILLIPS

GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: 866.252.0878

gklinger@milberg.com

Attorney for Plaintiff Jason Braun